IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**Case No. 1:16-CR-53**
HAMZA KOLSUZ	)	

MEMORANDUM OPINION

Defendant is charged in a three-count indictment with (i) attempting to export from the United States various firearms parts on the United States Munitions List ("USML") without a license, in violation of 22 U.S.C. § 2778, (ii) attempting to smuggle goods from the United States, in violation of 18 U.S.C. § 554(a), and (iii) engaging in a conspiracy to commit those offenses, in violation of 18 U.S.C. § 371. At issue is defendant's pre-trial motion to suppress evidence discovered as a result of the government's two warrantless searches of defendant's cell phone, which the government seized as defendant was about to board an airplane to leave the United States. The government first searched defendant's cell phone at the airport by reviewing the cell phone's most recent calls and text messages. Thereafter, following defendant's arrest, the government transported defendant's cell phone to an off-site facility and conducted an extensive forensic search of the information contained on the cell phone. Defendant's motion to suppress presents the following questions:

> (i) whether the search of defendant's cell phone conducted at the airport and the search of defendant's cell phone conducted at the off-site location qualify as border searches; and
>
> (ii) if so, whether both searches of defendant's cell phone qualify as routine border searches that do not require a warrant, probable cause, reasonable suspicion, or any level of individualized suspicion.

As the matter has been fully briefed and argued orally, it is now ripe for disposition.

I.[1]

On January 25, 2016, defendant, a Turkish citizen who speaks little English, entered the United States at Miami International Airport on a B2 visitor's visa.

Thereafter, on February 1, 2016, Charles Reich, the United States Customs and Border Protection ("CBP") Special Agent assigned to the New York Homeland Security Investigations ("HSI") Field Office, called CBP Supervisory Officer Mike Augustino and Special Agent Jay Culley, who were on duty at Washington Dulles International Airport ("Dulles"), and informed them (i) that defendant had previously been stopped at John F. Kennedy International Airport ("JFK") attempting to export items on the USML from the United States to the Republic of Turkey without an export license, (ii) that defendant was scheduled to fly from Dulles to Turkey the following day, February 2, 2016, and (iii) that at Dulles, defendant's checked bags should be searched to determine whether they contained any firearms parts.

Thereafter, Special Agent Reich sent a follow up email to Supervisory Officer Augustino and Special Agent Culley, providing them with (i) defendant's name, date of birth, and Turkish citizenship, (ii) the summary written by the CBP officer who interviewed defendant when he entered the United States on January 25, 2016, and (iii) defendant's flight itinerary. Gov. Ex. 1, Reich Email. The email also stated, "[n]ot sure how his English is, on 1/08/2013 (2013SZ003360701) he was stopped by CBP exodus team at jfk with gun parts. Had a Turkish speaking [CBP officer] on site." *Id.* In the same email, Special Agent Reich again asked Supervisory Officer Augustino and Special Agent Culley to examine defendant's checked bags

---

[1] The facts listed here are derived primarily from the parties' joint stipulation of facts and the government's supporting exhibits. This factual summary also benefits from the credible testimony of United States Customs and Border Protection Special Agent Adam Coppolo, presented during the April 29, 2016 hearing on defendant's motion to suppress.

to look for firearms parts. Special Agent Reich also requested that Supervisory Officer Augustino and Special Agent Culley ask defendant various questions.[2]

Shortly thereafter, Supervisory Officer Augustino forwarded Special Agent Reich's email to CBP's Tactical Terrorist Response Team ("TTRT") and the Counterterrorism Response Team at Dulles. Thereafter, TTRT Supervisory Officer Lauren Colgan assigned CBP Officer Jonathan Budd to the matter. Both Supervisory Officer Colgan and Officer Budd reviewed Special Agent Reich's email.

After reading Special Agent Reich's email, Supervisory Officer Colgan reviewed a CBP report summarizing the circumstances involved in the January 8, 2013 stop of defendant at JFK. This report disclosed:

> (i) that on January 8, 2013, a search of defendant's checked luggage revealed a Beretta .380 automatic pistol slide, a barrel, a guide rod, and a recoil spring;
>
> (ii) that the CBP detained the parts and referred the matter to the United States Department of State to determine whether the parts were on the USML; and
>
> (iii) that the parts were seized one week later after CBP was advised by the Department of State that the parts were listed on the USML and could not legally be exported from the United States without a license from the United States Department of State Directorate of Defense Trade Controls ("DDTC").

The CBP report also referred to an incident on December 2, 2012, in which firearms parts listed on the USML were found in defendant's luggage when he attempted to transport his luggage from the United States, through JFK, to Turkey without an export license from the Department of State. CBP agents seized these firearms parts. In addition to reviewing the CBP report,

---

[2] Specifically, Special Agent Reich asked Supervisory Officer Augustino and Special Agent Culley to ask defendant questions regarding (i) who defendant met in Florida, (ii) whether defendant received money from anyone, (iii) what tourist activities defendant engaged in during his visit, (iv) whether defendant attended a gun show in Ohio, (v) whether defendant purchased anything related to firearms, (vi) whether defendant shipped any parts out of the country, and (vii) whether anyone accompanied defendant in Ohio.

Supervisory Officer Colgan also reviewed TECS[3] records memorializing the December 2, 2012 and January 8, 2013 stops of defendant at JFK, which disclosed defendant's prior attempts to export firearms parts without a license.

On February 2, 2016, defendant began his return trip to Turkey by checking in at Miami International Airport for a series of flights that would take him and his checked luggage through Cleveland Hopkins International Airport and Dulles to Istanbul, Turkey. After defendant and his checked luggage arrived at Dulles, defendant's checked bags were removed from defendant's inbound United Airlines flight, but at Supervisory Officer Colgan and Officer Budd's instruction, the checked bags were not loaded onto defendant's outbound Turkish Airlines flight.

Once Supervisory Officer Colgan and Officer Budd obtained defendant's two pieces of checked luggage, they performed an outbound customs examination of the luggage and discovered various firearms parts. Specifically, the inspection revealed eighteen handgun barrels, twenty-two 9mm handgun magazines, four .45 caliber handgun magazines, and one .22 caliber Glock caliber conversion kit.[4] Based on their training and experience, Supervisory Officer Colgan and Officer Budd immediately knew that the barrels and the caliber conversion kit were listed on the USML, and therefore defendant could not lawfully remove these items from the United States without a DDTC export license.

After Supervisory Officer Colgan and Officer Budd discovered the firearms parts in defendant's checked luggage, Special Agent Culley arrived at Dulles. Shortly thereafter, Supervisory Officer Colgan, Officer Budd, Supervisory Officer Augustino, and Special Agent

---

[3] TECS is an internal database that serves as a data repository to support law enforcement "lookouts," border screening, and reporting of border inspection processes.

[4] Defendant's luggage also contained one .357 caliber handgun magazine, but it is unclear whether the CBP officers were aware of that fact at the time of the search.

Culley conducted an outbound customs inspection of defendant on the jetway as he attempted to board his flight to Istanbul. Although a CBP Turkish translator was not present during the outbound customs inspection, a Turkish Airlines representative acted as a translator.[5] During the outbound customs inspection, defendant admitted (i) that he was in possession of firearms parts, (ii) that he had initially flown into Miami and then travelled to Ohio, (iii) that while in Ohio, he attended a gun show where he made cash purchases of the firearms found in his checked luggage,[6] and (iv) that he did not have a federal firearms license for the firearms and was unware of any other licensing requirement. Defendant also noted that because he did not bring very much cash into the United States, he used his ATM cards to withdraw the cash needed to purchase the firearms parts found in his checked luggage. At the time of the encounter, defendant possessed approximately $2,600 in cash. Defendant claimed that he purchased the firearms parts for personal use and that he had no intention of selling them in Turkey or any other country.

On the jetway at Dulles, CBP officers took defendant's iPhone 6 Plus Model #A1524 ("iPhone") from his person and placed it in defendant's carry-on luggage. Defendant was then transported—along with his carry-on luggage—to the CBP secondary inspection area. There, Supervisory Officer Colgan used the iPhone's touch screen to navigate the iPhone's operating system—which was not password protected—to reveal defendant's most recent text messages and calls. No further inspection of defendant's iPhone was conducted at that time. Also in the secondary inspection area, Supervisory Officer Colgan used the Automated Export System

---

[5] The Turkish Airlines representative is not affiliated with CBP in any official manner, but that representative speaks Turkish and English as part of his job and has aided government agents with translation in the past.

[6] Contrary to defendant's statements on the jetway, defendant never visited a gun show in Ohio. Although defendant was briefly in Ohio on February 2, 2016, after flying from Miami, Florida to Cleveland Hopkins International Airport, he spent the entirety of his time in Ohio at the Cleveland Hopkins International Airport awaiting the departure of his flight to Dulles.

("AES"), a government database for information related to exports, to ascertain: (i) whether defendant had ever filed an export license with CBP at the time of any export, and (ii) whether defendant was listed as a license registrant with DDTC. The AES revealed no records associated with defendant.

CBP Special Agent Adam Coppolo then read defendant his *Miranda*[7] rights, and Special Agent Coppolo, Special Agent Culley, and CBP Special Agent James Donovan interviewed defendant. During the interview, defendant stated

> (i) that he entered the United States with the intention of sightseeing in Florida with a friend, Bayram Bulut, whom defendant has known since 2006 or 2007;
>
> (ii) that defendant was in possession of $9,000 in cash when he entered the United States;
>
> (iii) that defendant had visited numerous gun shops, pawn shops, and a gun show while he was in Florida;
>
> (iv) that defendant had purchased the firearms parts at the gun show in Florida;
>
> (v) that Bulut had not purchased any of the firearms parts;
>
> (vi) that no one had ordered the firearms parts found in his checked luggage; and
>
> (vii) that although Bulut cautioned defendant against purchasing gun parts, defendant did not heed Bulut's warning.

The agents ended the interview of defendant in the early morning on February 3, 2016. Shortly thereafter, the agents arrested defendant, and Special Agent Coppolo took custody of defendant's iPhone. The agents also seized handgun barrels, a handgun caliber conversion kit, magazines, laser aiming modules, and two pieces of luggage.

Thereafter, Special Agent Coppolo transported defendant's iPhone approximately four miles from Dulles to the HSI office in Sterling, Virginia. There, Special Agent Coppolo

---

[7] *Miranda v. Arizona*, 384 U.S. 436 (1966).

delivered defendant's iPhone to HSI Computer Forensic Agent Michael Del Vacchio and asked for his assistance in conducting a forensic search by extracting digital information from defendant's iPhone. When Forensic Agent Del Vacchio received defendant's iPhone, it was in airplane mode—meaning it could not access a cellular network or the Internet—and Forensic Agent Del Vacchio did not change this setting. Forensic Agent Del Vacchio connected the iPhone to a Cellebrite Physical Analyzer, a tool that extracts data from electronic devices, and conducted an advanced logical file system extraction, which copied data only from the iPhone's allocated space—space to which the phone's operating system had already written files. The Cellebrite software did not access any data stored remotely—or in the "cloud"—and instead accessed only data stored on the iPhone itself. Forensic Agent Del Vacchio did not make a complete bitstream copy of defendant's iPhone.[8]

Once the logical file system extraction was complete, the Cellebrite Physical Analyzer generated a 896-page report that Forensic Agent Del Vacchio subsequently provided to Special Agent Coppolo. The report includes the defendant's personal contact lists, photographs, videos, emails, and conversations with others using various messaging applications. The report also contains information from the iPhone's calendar, web browsing history, call logs, and physical location log, which reflected a history of the iPhone's precise GPS coordinates.

After reviewing the lengthy report, Special Agent Coppolo prepared a Report of Investigation ("ROI") regarding the search of defendant's iPhone. The report states:

> (i) that "[f]rom on or after February 2, 2016, to on or about March 3, 2016, a customs border search was conducted on [defendant's] cell phone";

---

[8] A bitstream copy obtains everything on a phone—including data from the phone's unallocated space. In other words, a bitsream copy extracts not only files saved and easily accessible on an electronic device, it also extracts residual data of files that have been deleted.

> (ii) that Special Agent Coppolo reviewed the Cellebrite report "to conduct a border search of the iPhone in order to search for violations of law, including but not limited to, violations of Title 22 United States Code Section 2778 and Title 18 United States Code Section 554";
>
> (iii) that "[f]rom on or about February 3, 2016 to on or about March 3, 2016, SA Coppolo accessed this [Cellebrite] report pursuant to customs border search authority" and that "[a]mong other things, SA Coppolo reviewed contact lists, emails, messenger conversations (including but not limited to Kik and iChat conversations), photos and videos"; and
>
> (iv) that on March 3, 2016, Special Agent Coppolo confirmed with Forensic Agent Del Vacchio that no other information could be obtained from the iPhone.

Gov. Ex., 7, ROI.

On March 3, 2016, after defendant had already been charged in a Criminal Complaint, a grand jury returned a three-count Indictment against defendant charging him with (i) attempting to export from the United States various firearms parts on the USML without a license, in violation of 22 U.S.C. § 2778, (ii) attempting to smuggle goods from the United States, in violation of 18 U.S.C. § 554(a), and (iii) engaging in a conspiracy to commit those offenses, in violation of 18 U.S.C. § 371. Thereafter, defendant filed a motion to suppress the evidence discovered as a result of the government's two warrantless searches of defendant's iPhone, namely (i) the initial search of the iPhone's recent calls and text messages conducted at the airport, and (ii) the forensic search conducted at the HSI office in Sterling, Virginia.

II.

It is now well-settled that border searches are an exception to the Fourth Amendment requirement that a search be supported by a warrant and probable cause. Specifically, under the border search exception, government agents may conduct "routine" searches and seizures of persons and property at the border without obtaining a warrant or establishing any level of individualized suspicion. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). As

the Supreme Court has explained, these searches are allowed because "[t]he [g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Moreover, although the government's interest is significant at the border, the individual's privacy interest is substantially lessened because "a port of entry is not a traveler's home." *United States v. Thirty-Seven (37) Photographs*, 402 U.S. 363, 376 (1971) (plurality opinion). In this regard, the Supreme Court has noted that an individual approaching the border should not be surprised that "[c]ustoms officers characteristically inspect luggage ... ; it is an old practice and is intimately associated with excluding illegal articles from the country." *Id.* Thus, it is well-established "[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

The border search exception applies to the international border and its "functional equivalent," including international airports. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973).[9] Moreover, although the Supreme Court has never squarely addressed whether the border search exception applies to individuals and objects *exiting* the United States, the Fourth Circuit has addressed this question and held that a border search "conducted upon a person *exiting* from the country" is "properly within the border search exception to the Fourth Amendment." *United States v. Oriakhi*, 57 F.3d 1290, 1297 (4th Cir. 1995) (emphasis in original).

---

[9] *See, e.g.*, *United States v. Lawson*, 461 F.3d 697, 700 (6th Cir. 2006) (holding that an international airport is the "functional equivalent" of the border); *United States v. Klein*, 592 F.2d 909, 911 n.1 (5th Cir. 1979) (same).

Accordingly, the question presented here is whether the two warrantless searches of defendant's iPhone—the initial inspection at the airport and the more sophisticated forensic search conducted off-site at the HSI office—qualify as routine border searches that do not require a warrant or individualized suspicion.

III.

Defendant first contends that the evidence discovered as a result of the government's second warrantless search of defendant's iPhone—the search conducted at the HSI office—must be suppressed because that search was not a border search, and therefore under the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014), the search of defendant's iPhone required a warrant and probable cause. *Id.* 2484-85, 2489-91 (2014) (holding that a search incident to arrest of a cell phone requires a warrant and probable because a search of the digital information contained on a cell phone is categorically different from a search of other personal effects). Specifically, defendant contends that the iPhone search conducted at the HSI office was not a border search because (i) the search occurred after defendant was arrested, and (ii) the search was spatially and temporally attenuated from the border search of defendant's other personal effects.

Yet, as the government correctly contends, defendant's argument fails in both respects. To begin with, contrary to defendant's contention, the fact of arrest does not abrogate the government's authority to complete a border search. The Fourth Circuit and other circuits have consistently held that the government may conduct a border search after arresting an individual. *See United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005) (holding that a post-arrest search of

defendant's laptop was a border search).[10] To conclude otherwise would be to encourage border agents to refrain from making a lawful arrest until after completing a border search in its entirety, a result that could place border agents and society in danger.

Moreover, the fact that the forensic search of defendant's iPhone occurred four miles from Dulles and was not completed until approximately one month after the phone was seized does not alter the conclusion that the search of defendant's iPhone was a border search. This is so because, as several courts have held, an off-site forensic search of an electronic device over a long period of time is nonetheless a border search where, as here, the electronic device was seized at the border, the device was never cleared to pass through the border, and therefore the defendant never "regain[ed] an expectation of privacy in [the electronic device]." *United States v. Stewart*, 729 F.3d 517, 526 (6th Cir. 2013).[11]

Thus, contrary to defendant's contention, the post-arrest, off-site forensic search of defendant's iPhone is not governed by *Riley*, but is instead a border search, which does not require a warrant supported by probable cause. Importantly, however, this conclusion does not end the analysis. It remains to be resolved whether the two searches of defendant's iPhone—the

---

[10] *See, e.g.*, *United States v. Calderon-Quinonez*, 382 F. App'x 540, 541 (9th Cir. 2010) (holding that the seizure of cocaine following an arrest was a valid border search); *United States v. Bates*, 526 F.2d 966, 967-68 (5th Cir. 1976) (concluding that a search of an individual's vehicle after the arrest of that individual was a valid border search). *But see United States v. Caballero*, No. 15cr2738-BEN, 2016 WL 1546731, at *5-7 (S.D. Cal. Apr. 14, 2016) (holding that under Ninth Circuit precedent, a post-arrest search of a cellphone was a valid border search that required reasonable suspicion, but noting in dictum that *Riley* may compel the conclusion that a post-arrest search of a cell phone at the border requires a warrant and probable cause).

[11] *See also United States v. Cotterman*, 709 F.3d 952, 961-62 (9th Cir. 2013) (en banc) (concluding that a search of defendant's laptop that was seized at the border and examined 170 miles away in a specialized lab was a border search because the laptop was seized at the border and had not been cleared to pass through the border); *United States v. Feiten*, No. 15-20631, 2016 WL 894452, at *2 (E.D. Mich. March 9, 2016) (holding that an off-site, month-long forensic search of a laptop was a border search).

initial search conducted at the airport and the forensic search conducted off-site at the HSI office—were routine border searches or nonroutine border searches.

IV.

Defendant next contends that the evidence obtained as a result of searching defendant's iPhone must be suppressed because both searches of defendant's iPhone were nonroutine border searches that required some level of individualized suspicion. In response, the government contends (i) that both searches of defendant's iPhone were routine border searches, and (ii) even assuming the searches were nonroutine, the government had sufficient individualized suspicion to conduct both searches.

A.

The Supreme Court has made clear that under the border search exception, only routine border searches are wholly immune from the typical Fourth Amendment requirements, whereas nonroutine border searches must rest on some degree of particularized suspicion. *Montoya de Hernandez*, 473 U.S. at 541. Although the Supreme Court has not often addressed the distinction between routine and nonroutine searches, it has provided some guidance for determining what constitutes a routine search. On the one hand, in *United States v. Flores-Mantano*, the Supreme Court held that "the [g]overnment's authority to conduct [routine] suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank." 541 U.S. at 155. In reaching this conclusion, the Supreme Court determined (i) that an individual's privacy interest in the contents of a vehicle's gas tank was less than an individual's privacy interest in the contents of a vehicle's passenger compartment, (ii) that such searches of a vehicle's gas tank were relatively brief, and (iii) that the possibility of permanent damage to a car was remote. *Id.* at 154-55.

On the other hand, in *United States v. Montoya de Hernandez*, the Supreme Court determined that a seizure "beyond the scope of a routine customs search and inspection" occurred when the defendant was detained at the border for sixteen hours after she declined to be x-rayed and to produce a monitored bowel movement because custom officials suspected that defendant had swallowed balloons of cocaine in an effort to smuggle drugs across the border. 473 U.S. at 532-36, 541. After a sixteen-hour detention, border officials obtained a court order to conduct a rectal examination, which disclosed balloons of cocaine in the defendant's bowel. *Id.* at 535-36. The Supreme Court held that the seizure was not routine, but nonetheless concluded that the nonroutine seizure was constitutional because it was justified by the customs officials' reasonable suspicion that the defendant was smuggling drugs in her alimentary canal. *Id.* at 541.

Although the Supreme Court has not made pellucid exactly what renders a border search nonroutine—and what level of individualized suspicion is necessary for nonroutine searches—circuit courts have looked to the intrusiveness of the search in distinguishing between routine and nonroutine border searches. *See, e.g.*, *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006) ("[T]he level of intrusion into a person's privacy is what determines whether a border search is routine.").[12] In this regard, circuit courts have consistently held that searches of an individual's outer clothing, luggage, and personal effects are routine searches,[13] whereas more physically intrusive searches—such as strip searches, alimentary canal searches, x-rays, and the removal of

---

[12] *See also United States v. Braks*, 842 F.2d 509, 512 (1st Cir. 1988) (applying several factors to determine whether a search is sufficiently intrusive to be a nonroutine border search).

[13] *See, e.g.*, *United States v. Johnson,* 991 F.2d 1287, 1291-92 (7th Cir. 1993) (holding that "the search of a border entrant's suitcase, purse, wallet, and overcoat simply is not sufficiently intrusive to be considered nonroutine"); *United States v. Ezeiruaku*, 936 F.2d 136, 140-41(3d Cir. 1991) (holding that examination of luggage at the border was routine); *United States v. Benevento*, 836 F.2d 60, 68 (2d Cir. 1987) (same).

an artificial limb—are nonroutine searches requiring particularized reasonable suspicion.[14] Less clear, however, is whether digital searches of electronic devices—such as computers and cell phones—count as routine border searches.

In this regard, the Fourth Circuit in *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), addressed a digital border search of an electronic device. There, as part of a routine border inspection, the government discovered, *inter alia*, a video camera with "a tape of a tennis match which focused excessively on a young boy" and "several albums containing photographs of provocatively-posed prepubescent boys, most nude or semi-nude." *Id.* at 502, 503. The government agents arrested the defendant, and continued to search the van, discovering a computer and approximately seventy-five disks. *Id.* After seizing the computer and disks, government agents searched the contents of these electronic devices and found that they contained child pornography. *Id.* Specifically, government agents manually investigated the contents of the computer and the disks by accessing their content in the same way a typical user would do so; the government did not conduct a sophisticated forensic analysis of the contents of the computer and the disks. *Id.* The Fourth Circuit in *Ickes* held that the manual digital border search of the computer and disks was routine, and therefore did not require any level of suspicion. *Id.* at 505-06. The Fourth Circuit reached this conclusion by comparing computer files to the physical contents of any other "cargo" subject to a routine search and inspection at the border. *Id.* at 504. In this regard, the Fourth Circuit held that a manual review of electronic files

---

[14] *See, e.g.*, *United States v. Uricoechea-Casallas*, 946 F.2d 162, 166 (1st Cir. 1991) (applying a "reasonable suspicion" standard to a strip search at the border); *Rivas v. United States*, 368 F.2d 703, 710 (9th Cir. 1966) (holding that an alimentary canal search was a nonroutine border search); *United States v. Vega-Barvo*, 729 F.2d 1341, 1349 (11th Cir. 1984) (holding that an x-ray was a nonroutine border search); *United States v. Sanders*, 663 F.2d 1, 3 (2d Cir. 1981) (holding that removal of artificial limb was a nonroutine border search).

contained on a computer is no different than a manual review of papers contained in luggage, a classic example of a routine border search. *Id.* at 505-06.[15]

Although *Ickes* clearly stands for the proposition that a manual digital search of an electronic device is a routine border search, that decision does not address whether more sophisticated forensic searches of electronic devices at the border may properly be classified as routine border searches. In this regard, a district court in this circuit recently addressed whether a forensic search of a cell phone is a routine border search. *See United States v. Saboonchi*, 990 F. Supp.2d 536, 560 (D. Md. 2014). In *Saboonchi*, border agents confiscated two cell phones and a flash drive after stopping the defendant and his wife at the border. *Id.* at 539. The border agents searched both cell phones by creating " 'a perfect bitstream copy' "—a complete copy—" 'of the original storage device' " and then using "specialized software to comb through the data ... searching the full contents of the [copied] hard drive, examining the properties of individual files, and probing the drive's unallocated 'slack space' to reveal deleted files." *Id.* at 547 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 540 (2005)). The government argued that under *Ickes*, the forensic searches were routine border searches, and therefore not subject to a reasonable suspicion requirement. *Id.* at 544, 546. But the court in *Saboonchi* distinguished *Ickes* on the ground that *Ickes* involved a manual digital search, whereas the search at issue in *Saboonchi* was a forensic digital search. *Id.* at 546.[16] Thus, the

---

[15] *See also United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that a manual search of a computer's contents was a routine border search because it was no different than a manual search of physical luggage).

[16] In this regard, the court in *Saboonchi* noted (i) that "an integral part of a forensic examination is the use of technology-assisted search methodology, where the computer searches vast amounts of data that would exceed the capacity of a human reviewer to examine in any reasonable amount of time," and (ii) that "[t]he techniques used during a forensic search can be distinguished from a conventional computer search"—such as the manual search at issue in *Ickes*—"in which a

district court in *Saboonchi* concluded that the holding of *Ickes* was limited to manual digital border searches of electronic devices, and hence did not apply to significantly more intrusive forensic digital searches. *Id.* at 569. Ultimately, the court in *Saboonchi* held that forensic digital searches are nonroutine border searches, and therefore reasonable suspicion is required, on the ground that "[i]t is difficult to conceive of a property search more invasive or intrusive than a forensic computer search—it essentially is a body cavity search of a computer." *Id.* at 569.

Although the line between routine and nonroutine border searches remains somewhat indistinct, the juxtaposition of the two searches of defendant's iPhone well-illustrates where the dividing line exists with respect to the border searches of electronic devices. The first of these searches—the manual inspection of text messages and recent calls on defendant's iPhone conducted at the aiport—is clearly a routine border search under the Fourth Circuit's decision in *Ickes*. 393 F.3d at 505-06. This search, like the search in *Ickes*, was conducted by accessing the content of defendant's iPhone in the same manner as a typical user, namely by using the touch screen to navigate the phone's operating system to reveal defendant's recent text messages and calls. *Id.* at 503. Thus, the manual search of defendant's iPhone conducted at the aiport was a routine border search that did not require individualized suspicion.

Importantly, however, *Ickes* does not dictate the outcome with respect to the second, significantly more extensive forensic search of defendant's iPhone. Unlike in *Ickes*, in conducting the forensic search here, government agents (i) seized defendant's iPhone, (ii) moved the iPhone to an off-site location, (iii) used the Cellebrite Physical Analyzer to perform a logical file system extraction of the hard drive's allocated space, and (iv) used the Cellebrite Physical Analyzer to generate an 896-page report that includes, *inter alia*, information from defendant's

---

Customs officer may operate or search an electronic device in much the same way that a typical user would use it." *Id.* at 547.

contact lists, photographs, videos, emails, web browsing history log, and physical location log. Thus, it remains to be determined whether the off-site forensic search of defendant's iPhone was a nonroutine border search that required some level of individualized suspicion.

In addressing this question, it is appropriate to consider the Supreme Court's decision in *Riley*. Although that decision does not specifically address a search of a cell phone conducted at the border, the Supreme Court in *Riley* made clear that cell phones are categorically different from other personal effects, such as containers. 134 S. Ct. at 2484-85, 2489-91. Specifically, in light of the "immense storage capacity" of modern cell phones and the variety of information stored on cell phones, the Supreme Court concluded that "a cell phone would typically expose to the government far more than the most exhaustive search of a house." *Id.* at 2489, 2491.[17] Accordingly, the Supreme Court in *Riley* concluded that to allow officers to conduct a warrantless search of a cell phone incident to arrest "would untether" the search incident to arrest exception "from the [historical] justifications underlying [the doctrine]," namely officer safety and preventing the destruction of evidence. *Id.* at 2485.

Since the Supreme Court's decision in *Riley*, at least two district courts—but no circuit courts—have squarely addressed whether the rationale of *Riley* is relevant in analyzing whether a border search of an electronic device, such as a laptop or a cell phone, is a routine or nonroutine border search. *See United States v. Kim*, 103 F. Supp.3d 32, 54-59 (D. D.C. 2015); *United States*

---

[17] Indeed, the Supreme Court in *Riley* noted that the suggestion that a data search of a cell phone is "materially indistinguishable" from searches of physical items was "like saying a ride on horseback is materially indistinguishable from a flight to the moon" because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 2488-89.

v. Feiten, No. 15-20631, 2016 WL 894452, at *4-7 (E.D. Mich. March 9, 2016).[18] The court in *Kim* held that in light of *Riley*, an off-site extensive forensic search of an electronic device is a nonroutine border search that requires some level of individualized suspicion because an individual's privacy interest implicated by such a search outweighs the government's interest in conducting a forensic search of a cell phone at the border. 103 F. Supp.3d at 56-57. In contrast, the court in *Feiten* held that an extensive forensic search of an electronic device is a routine border search that does not require individualized suspicion because although "[l]aptops and cell phones may be new and increasingly capacious containers, searching the effects, digital or otherwise, of those who present themselves at the international border for inspection is an old practice ... intimately associated with excluding illegal articles from the country." 2016 WL 894452, at *6 (internal quotation marks omitted).

Although the courts in *Kim* and *Feiten* reached different results, both courts agreed that in considering the question whether *Riley* compels a conclusion that an offsite forensic search of an electronic device was a nonroutine border search, it is appropriate to "assess[], on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interest," and as part of that assessment, it is appropriate to consider whether a particular application of the border

---

[18] It is also worth noting that the court in *Saboonchi* addressed on a motion for reconsideration the question whether the Supreme Court's decision in *Riley* affected its prior ruling that a forensic digital search of a cell phone was a nonroutine border search. *United States v. Saboonchi*, 48 F. Supp.3d 815, 816 (D. Md. 2014). The court in *Saboonchi* denied the defendant's motion for reconsideration on two grounds: (i) that the Supreme Court in *Riley* did not explicitly rule on the border search exception, and (ii) that in any event, the district court's prior holding that a forensic digital search of a cell phone was nonroutine was consistent with the principles the Supreme Court outlined in *Riley*. *Id.* at 816.

search exception would "untether the rule from the justifications underlying the [border search] exception." *Riley*, 134 S. C.t at 2484, 2485 (internal quotation marks and citations omitted).[19]

It is appropriate to apply the same analytical framework here. With respect to the privacy concerns involved, an individual's privacy interest in the information contained on his cell phone is much greater than an individual's privacy interest in the contents of his luggage or other personal effects. Indeed, a cell phone cannot fairly be compared to an ordinary container that might be searched at the border because as the Supreme Court in *Riley* made clear, "[a] phone not only contains in digital form many sensitive records previously found in the home," but also "a broad array of private information never found in a home in any form—unless the phone is [in the home]." *Id.* at 2491.[20] As one court has noted, "[i]t is difficult to conceive of a property search more invasive or intrusive" than a sophisticated, digital search of a cell phone because such a search is "essentially [] a body cavity search" of the cell phone. *Saboonchi*, 990 F. Supp.2d at 569. Thus, even at the border, an individual has a significant privacy interest in the digital contents of his cell phone.

In opposition to the conclusion that an individual has a significant privacy interest in the digital contents of a cell phone, the government contends that the forensic search of defendant's iPhone was not as extensive as it could have been. In support of this argument, the government

---

[19] *Kim*, 103 F. Supp.3d at 55 ("[F]ollowing the approach utilized in *Riley*, the Court must proceed 'by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."); *Feiten*, 2016 WL 894452, at *5 ("The appropriate application of *Riley* to the instant case, therefore, is to determine whether allowing agents to forensically search an entrant's laptop without [some individualized suspicion] would necessarily untether *that* rule from the historical justifications underlying it.") (emphasis in original).

[20] In this respect, it is worth noting that to the extent the court in *Feiten* analyzed cell phone searches at the border by comparing cell phones to containers, 2016 WL 894452, at *5, the analysis was inconsistent with the Supreme Court's conclusion in *Riley* that cell phones are categorically distinct from other containers. 134 S. Ct. at 2488-89.

points out that the forensic search in issue here, unlike the search in *Saboonchi*, did not involve a complete bitstream copy of both the allocated and unallocated space on the cell phone's hard drive and the use of keywords to search the copied drive for specific information. 990 F. Supp. at 539. In other words, the government attempts to distinguish an extensive forensic search of a cell phone from a *very* extensive forensic search of a cell phone. This argument fails because it draws too fine a distinction. The forensic search in issue here was not as extensive as the forensic search in *Saboonchi*, to be sure, but both searches involved the use of specialized software to copy a large amount of data from an individual's cell phone. It is not significant that the forensic search in *Saboonchi* involved the copying of all the data contained on a cell phone's hard drive, whereas the forensic search in issue here involved only the copying of the allocated space on the iPhone's hard drive. The data copied here was substantial enough to fill 896 printed pages with information concerning defendant's contacts, his correspondence, his schedule, the phone's web browsing history, the phone's call logs, and a physical location log, which reflected a history of defendant's precise GPS coordinates. As the Supreme Court in *Riley* noted, such an immense amount of disparate personal information allows the government to reconstruct "an individual's private life." *Riley*, 134 S. Ct. at 2489. Thus, although the forensic search of defendant's iPhone did not involve the copying of every bit of data contained on the phone's hard drive, it nonetheless implicated significant privacy interests. To suggest otherwise is like suggesting that a strip search does not implicate a significant privacy interest so long as the government does not look between the person's toes.

The government, as a sovereign, also has a significant interest at the border in protecting its territory and national security "by stopping and examining persons crossing into this country." *Ramsey*, 431 U.S. at 616. These significant governmental interests justify a wide range of

warrantless border searches. *Id.* Importantly, however, as the district court in *Kim* recognized, although "there is [circuit court] authority that states that the government's broad authority at the border extends to those exiting the country as well as those coming in," the Supreme Court has consistently justified the government's interests at the border "in terms of threats posed at the point of *entry*." *Kim*, 103 F. Supp.3d at 56 (emphasis added).[21] In this regard, none of the significant government interests in monitoring what *enters* the country applies where, as here, the object of a warrantless border search was *exiting* the country.[22] Of course, the government has an interest that justifies some suspicionless border searches of *departing* persons and their effects, namely potential violations of the export control laws.[23] But this interest is not directly implicated where, as here, a government agent conducts a forensic search of a cell phone, as the digital contents of a cell phone are not banned by export control regulations. This is not to say that digital information contained on a cell phone will not be useful in discovering illegally

---

[21] *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 537 (noting that the border search exception is justified on the basis of "regulat[ing] the collection duties and ... prevent[ing] the introduction of contraband into this country."); *Ramsey*, 431 U.S. at 620 ("The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."); *Thirty-Seven Photographs*, 402 U.S. at 376 ("Customs officials characteristically inspect luggage and their power to do so is not questioned ... ; it is an old practice and is intimately associated with excluding illegal articles from the country."); *Carroll v. United States*, 267 U.S. 132, 154 (1925) ("Travelers may be [stopped and searched] in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belonging as effects which may be lawfully brought in.").

[22] This conclusion distinguishes the present case from *Feiten*, in which the court held that the government's interest in searching the cell phone of a traveler *entering* the United States was significant because " '[t]he [g]overnment's interest *in preventing the entry of unwanted persons and effects* is at its zenith at the international border.' " 2016 WL 894452, at *5 (quoting *Flores-Montano*, 541 U.S. at 152) (emphasis in original).

[23] *See, e.g.*, *United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003) (finding that a border search of a large cargo container before it left the country was routine because "the United States' interest in preventing the export of weapons to other countries also implicates the sovereign's interest in protecting itself").

exported goods; indeed, such information will often be quite useful. For example, as the government notes, a cell phone may contain digital receipts of weapons parts purchases, images of weapons parts, or other information related to things an individual seeks to export illegally. Yet, all of this information is merely indirect evidence of the things an individual seeks to export illegally—not the things themselves—and therefore the government's interest in obtaining this information is less significant than the government's interest in directly discovering the items to be exported illegally.

Moreover, it is worth noting that any digital information contained on a cell phone that is relevant to exporting goods illegally can be easily obtained once a border agent establishes some level of individualized suspicion. And in the absence of some individualized suspicion that an individual seeks to export items illegally, there is little, if any, justification for a forensic search of a cell phone belonging to a traveler exiting the United States. This is especially true where, as here, the government has already arrested the defendant, seized his phone, and transported the phone to a secure location for further analysis.

In sum, although the manual search of defendant's iPhone conducted at the airport was a routine border search, the subsequent forensic search of defendant's iPhone conducted at the HSI office in Sterling, Virginia was a nonroutine border search requiring some level of individualized suspicion.

B.

It is next appropriate to consider what level of particularized suspicion is required to conduct a nonroutine border search of a cell phone. Defendant contends that the forensic search of his iPhone required a warrant supported by probable cause. Yet, defendant cites no case—nor have any been found—that stands for the proposition that more than reasonable suspicion is

required for a nonroutine border search or seizure of any kind or extent. Indeed, even where physically intrusive body searches have been in issue, courts have consistently held that no more than reasonable suspicion is required.[24] Thus, although the Supreme Court's decision in *Riley* appears to indicate that cell phones deserve the highest level of Fourth Amendment protection available, the highest protection available for a border search is reasonable suspicion. Accordingly, a nonroutine border search of a cell phone is constitutional if it is supported by reasonable suspicion.

The Supreme Court has defined reasonable suspicion as "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *United States v. Cortez*, 449 U.S. 411, 417-18 (1981). The standard is met when a law enforcement officer can point to "specific and articulable facts" and rational inferences that can be drawn from those facts indicating that criminal activity "may be afoot." *Terry v. Ohio*, 392 U.S. 1 (1968). A court's determination in this regard must be based upon the totality of the circumstances. *United States v. Arvizu*, 534 U.S. 266, 273 (2002). Importantly, as the Supreme Court has made clear, the reasonable suspicion standard relates to ongoing or imminent crime. *See Cortez*, 449 U.S. at 417 ("An investigatory stop must be justified by some objective manifestation that the person stopped is, or is about to be, engaged in criminal activity."). Accordingly, the question presented here is whether prior to the forensic search of defendant's iPhone, a reasonable officer could point to specific and articulable facts to support a conclusion that there was reasonable suspicion that defendant was engaged in ongoing criminal activity.

---

[24] *See, e.g.*, *Uricoechea-Casallas*, 946 F.2d at 166 (noting that a "reasonable suspicion" standard applies to a strip search at the border); *Rivas*, 368 F.2d at 710 (holding that an alimentary canal search is a nonroutine border search that requires some particularized suspicion); *Vega-Barvo*, 729 F.2d at 1349 (holding that an x-ray is a nonroutine border search that requires reasonable suspicion); *Sanders*, 663 F.2d at 3 (holding that removal of artificial limb is nonroutine border search that requires some particularized suspicion).

Here, the government had more than reasonable suspicion that defendant was attempting to export weapons parts listed on the USML without a license, in violation of the Arms Export Control Act, 22 U.S.C. § 2778. Specifically, prior to the search of defendant's iPhone, Special Agent Reich informed Supervisory Officer Augustino and Special Agent Culley:

> (i) of defendant's name, date of birth, and citizenship,
>
> (ii) that defendant had previously been stopped at JFK attempting to export items on the USML from the United States to Turkey without a license,
>
> (iii) about the summary that had been written by the CBP officer who interviewed defendant when he entered the United States on January 25, 2016, and
>
> (iv) that defendant was scheduled to take a flight from Dulles to Turkey on February 2, 2016.

Supervisory Officer Colgan and Officer Budd were also aware of this information, as they had reviewed Special Agent Reich's email. In addition, Supervisory Officer Colgan reviewed the CBP report that summarized the January 8, 2013 stop of defendant at JFK. And Supervisory Officer Colgan reviewed TECS records memorializing the December 2, 2012 and January 8, 2013 stops of defendant at JFK, which disclosed defendant's prior attempts to export firearms parts without a license. Moreover, prior to both searches of defendant's iPhone, the outbound customs exam of defendant's two pieces of checked luggage revealed various firearms parts listed on the USML, and defendant admitted on the jetway that he did not have the requisite DDTC license to export these items. Thereafter, Supervisory Officer Colgan used the AES to confirm (i) that defendant had never filed an export license with CBP at the time of any export, and (ii) that defendant was not listed as a license registrant with the DDTC.

Given these facts, government agents reasonably suspected that they would discover information on defendant's iPhone related not only to attempted export violations they had already discovered, but perhaps also information related to other ongoing attempts to export

illegally various firearms parts. Specifically, government agents reasonably suspected that defendant's iPhone contained digital receipts of weapons parts purchases, images of weapons parts, or other information related to items an individual seeks to export illegally. In addition, government agents could have reasonably suspected that defendant's iPhone contained information that would reveal the identity of co-conspirators, some of whom may have been attempting to smuggle firearms parts out of the country in the imminent future.

Thus, prior to conducting the off-site forensic search of defendant's iPhone, the border officials clearly had a "particularized and objective basis for suspecting" defendant of attempting to commit an ongoing or imminent crime. *Cortez*, 449 U.S. at 417. Indeed, in light of the extensive evidence the border agents had already discovered, even if probable cause were required here—which it is not—the government agents had sufficient evidence to meet that higher standard.

In sum, the two searches of defendant's iPhone were reasonable under the Fourth Amendment because the first search—the manual search conducted at the airport—was a routine border search that did not require any level of individualized suspicion, and the second search—the forensic search conducted at the HSI office—was a nonroutine border search justified by more than reasonable suspicion.

V.

Accordingly, for these reasons, defendant's motion to suppress the evidence obtained as a result of the government's two searches of defendant's iPhone must be denied.

An appropriate Order has already issued.

/s/
T. S. Ellis, III
United States District Judge

Alexandria, Virginia
May 5, 2016